Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Previously presented) A method for rollover of cryptographic keys during operation of a computer system, the method comprising:

providing an old set of cryptographic keys comprising at least a first cryptographic key and a second cryptographic key, wherein the first cryptographic key protects an integrity of secret information stored in a database and the second cryptographic key protects access to the secret information stored in the database;

checking with a key repository to determine if a certificate re-issuance is necessary, meanwhile maintaining the availability of the old set of cryptographic keys;

performing a rollover operation;

if the rollover operation results in new or revised keys, storing the new or revised keys in the database; and

if the rollover operation results in the new or revised keys, providing the new or revised keys to applications that need them when next requested by such applications.

2. (Previously presented) The method of claim 1, wherein checking with the key repository comprises utilizing one or more services of a specialized application acting as an extension of the key repository.

3. (Previously presented) The method of claim 2 wherein:

utilizing the one or more services of the specialized application comprises authenticating authorization of the specialized application to perform the one or more services.

4. (Original) The method of claim 1 being invoked as a result of a command.

5. (Original) The method of claim 1 being invoked as a result of a periodic check which senses that the old set of cryptographic keys are approaching expiration.

6. (Original) The method of claim 1 being invoked as a result of sensing an expired key.

7. (Original) The method as in claim 1, wherein the applications are notified of the presence of new keys by the Key Repository process.

8. (Original) The method as in claim 1, wherein the applications detect a missing key, and check with the Key Repository for that key and, if the missing key has been reissued, the applications receive a newly-issued key.

9. (Original) The method as in claim 1, wherein the Key Repository process is prompted by the applications to invoke the method as a result of the applications detecting a key approaching expiration.

10. (Original) The method as in claim 1, wherein the applications request the Key Repository process to provide thereto a new or revised key as a result of the applications detecting an expired key.

11. (Previously presented) A system, comprising:

a key repository configured to maintain at least a first key and a second key; and

a database coupled to the key repository and storing secret information, wherein the first key protects an integrity of the secret information stored in the database and the second key protects access to the secret information stored in the database.

12. (Previously presented) The system of claim 11 further comprising at least one application that can access the key repository, wherein the at least one application is pre-authorized to access the second key and can perform at least one function using the secret information without user intervention.

13. (Previously presented) The system of claim 11 wherein the database comprises entries defining at least one user of a first group of users and at least two users of a second group of users.

14. (Previously presented) The system of claim 13 wherein the first key has a value that is based on a password associated with the first group of users.

15. (Previously presented) The system of claim 13 wherein the second key has a value that comprises a plurality of value shares and wherein each value share is based on a password associated with the second group of users.

16. (Previously presented) The system of claim 13 wherein a value associated with at least one of the first key and the second key is changed when at least one event occurs, the at least one event selected from a group of events consisting of:

a user of the first group of users being added;
a user of the first group of users being deleted;
a user of the second group of users being added;
a user of the second group of users being deleted;
an algorithm used by the system being changed; and
the database being rewritten.

17. (Previously presented) The system of claim 13 wherein the key repository is configured to provide access to the second key in response to receiving a threshold number of valid passwords, each password associated with a different user from the second group of users.

18. (Previously presented) The system of claim 17 wherein the second key permits modification of at least one security parameter selected from the group consisting of:

a threshold number of valid passwords required to access the second key;

users assigned to the first group of users;

users assigned to the second group of users;

pre-authentication of an application to access at least one of the first key and the second key without user intervention;

cryptographic algorithms used by the system; and

pre-authentication of a program to act as an extension of the key repository.

19. (Previously presented) The system of claim 11 wherein the first key is used to encrypt a public key of an encryption algorithm.

20. (Previously presented) The system of claim 19 wherein the public key is used to encrypt a value associated with the first key and values shares associated with the second key.

21. (Previously presented) A method for rollover of cryptographic keys during operation of a computer system, the method comprising:

providing an old set of cryptographic keys comprising at least a first cryptographic key and a second cryptographic key, wherein the first cryptographic key protects an integrity of secret information stored in a database and the second cryptographic key protects access to the secret information stored in the database;

checking with a key repository to determine if a certificate re-issuance is necessary, meanwhile maintaining the availability of the old set of cryptographic keys;

performing a rollover operation;

if the rollover operation results in new or revised keys, storing the new or revised keys in the database; and

if the rollover operation results in the new or revised keys, providing the new or revised keys to applications that need them when next requested by such applications,

wherein the applications detect a missing key, and check with the Key Repository for that key and, if the missing key has been reissued, the applications receive a newly-issued key.